OSSライセンスチェッカー FOSSology と Linux

ソニー株式会社　布施　博明
2017.6.23

Agenda

- **自己紹介**
- **概要**
- **背景・前提**
  - OSS ライセンスとは
  - OSS ライセンストップ10
- **本題**
  - Sony 機器向け Linux における OSS のライセンス対応(GPLv3/LGPLv3)
  - FOSSology とは
  - FOSSology によるライセンス調査の実際
  - FOSSology で GPLv2 な OSS に GPLv3 ファイル混入を見つけたケース
- **まとめ**

Agenda

- **自己紹介**
- **概要**
- **背景・前提**
  - OSS ライセンスとは
  - OSS ライセンストップ10
- **本題**
  - Sony 機器向け Linux における OSS のライセンス対応(GPLv3/LGPLv3)
  - FOSSology とは
  - FOSSology によるライセンス調査の実際
  - FOSSology で GPLv2 な OSS に GPLv3 ファイル混入を見つけたケース
- **まとめ**

自己紹介

- 1991年ソニー入社
- NEWS ソフトウェア開発(BSD, System V)
- MemoryStick
- Media Cruising プロトコル開発(Free BSD)
- PS2 development tool ソフトウェア開発(Red Hat)
- PS2 Linux (Kondara)
- Sony 機器向け Linux (MontaVista)
- PS3 Linux ブートローダ/Linux (Fedora)
- Sony 機器向け Linux (独自)
- Sony 機器向け Linux (Ubuntu 14.04.x)

Sony が Linux を活用するためにやっている事

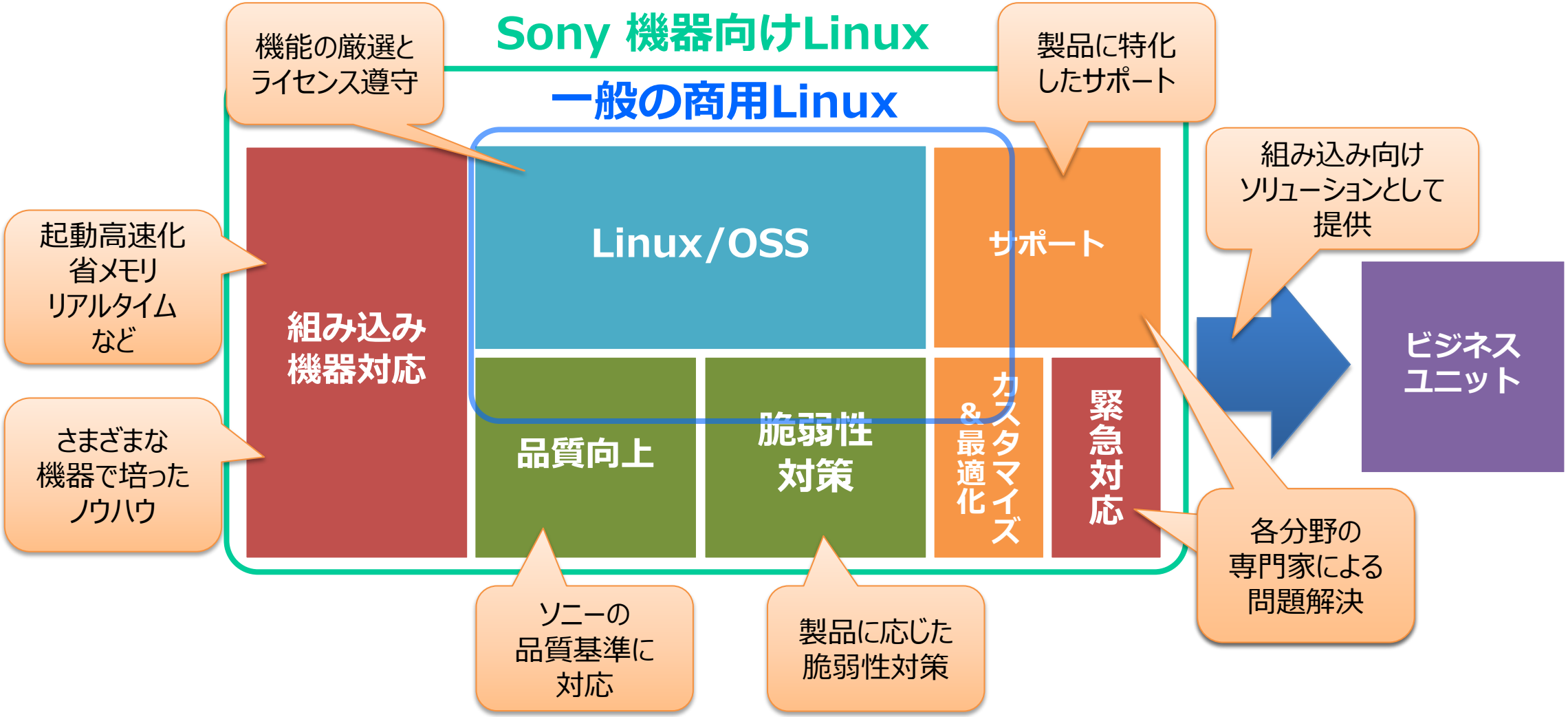
- **オープンソースソフトウェア (OSS) に各種品質向上を実施**
  - OSSそのままでは、実際の（ソニーの品質基準に対応した）商品化の際に課題が多い
  - **ソニーの品質基準に対応**し、多くの実績を持つ品質向上・安定化を実施
  - **商品に必要な機能をベースに厳選**した各種ソフトウェアパッケージとその品質管理
  - **OSSライセンス**を配慮したパッケージ選択
- **継続的な脆弱性監視と情報＆修正プログラムの提供**
  - **「脆弱性監視チーム」**を設置
  - セキュリティ対策も確実に実施

■追加開発

- **組み込み機器対応技術**を追加実装:
  - 起動高速化、サクサク化
  - 省メモリ化・省電力化
  - デバッグ・解析機能追加
  - RTパッチの適用、安定化
  - etc.

- **Linuxエキスパートによる技術サポート**
  - カーネル系、ユーザランド/コンパイラ系、デバイス系等、**各分野の専門家によるサポート・問題解決**の実施

Sony 機器向け Linuxと他のLinuxとの比較



Sony 機器の Linux 導入事例

最近の事例

Future Lab Program N

CES 2017 で展示

http://www.futurelab.sony.net/N/

α9

2017年5月26発売

http://www.sony.jp/ichigan/products/ILCE-9/index.html

Agenda

- **自己紹介**
- **概要**
- **背景・前提**
  - OSS ライセンスとは
  - OSS ライセンストップ10
- **本題**
  - Sony 機器向け Linux における OSS のライセンス対応(GPLv3/LGPLv3)
  - FOSSology とは
  - FOSSology によるライセンス調査の実際
  - FOSSology で GPLv2 な OSS に GPLv3 ファイル混入を見つけたケース
- **まとめ**

概要

- OSSを取り扱う上で必要なライセンスに関する背景・前提を説明する
- Sony 機器向け Linux におけるOSSライセンス対応について報告する

Agenda

- **自己紹介**
- **概要**
- **背景・前提**
  - OSS ライセンスとは
  - OSS ライセンストップ10
- **本題**
  - Sony 機器向け Linuxにおける OSS のライセンス対応(GPLv3/LGPLv3)
  - FOSSology とは
  - FOSSology によるライセンス調査の実際
  - FOSSology で GPLv2 な OSS に GPLv3 ファイル混入を見つけたケース
- **まとめ**

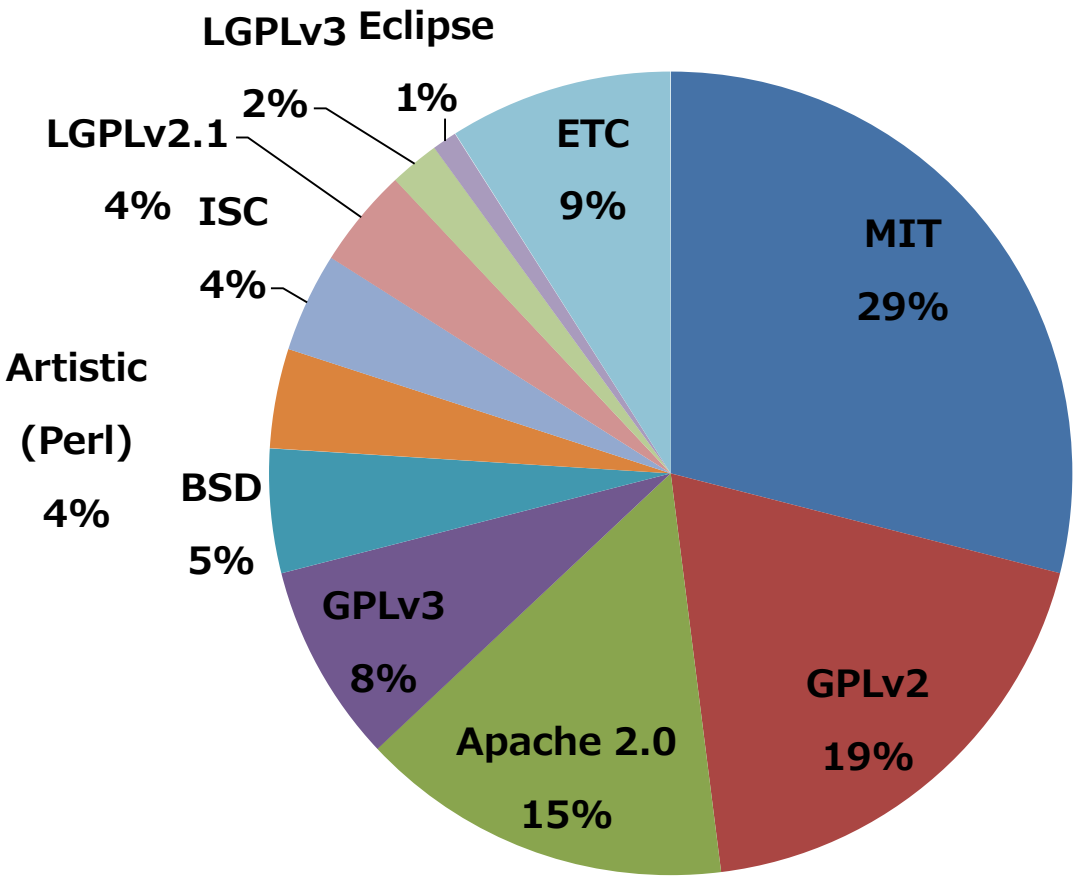
OSSライセンスとは

- **OSS（オープンソースソフトウェア）を利用する上で遵守すべき使用条件（利用許諾条件）**

- **ソニーの取り組み**
  - オープンソースソフトウエアライセンス取り扱いガイドライン

- **OSSが無料で使える ≠ 無条件で使える**
  - ライセンスに対する正しい理解と適切な対応が必要

OSS ライセンストップ 10



Rank	License	%
1	MIT	29
2	GPLv2	19
3	Apache 2.0	15
4	GPLv3	8
5	BSD	5
6	Artistic (Perl)	4
7	ISC	4
8	LGPLv2.1	4
9	LGPLv3	2
10	Eclipse	1

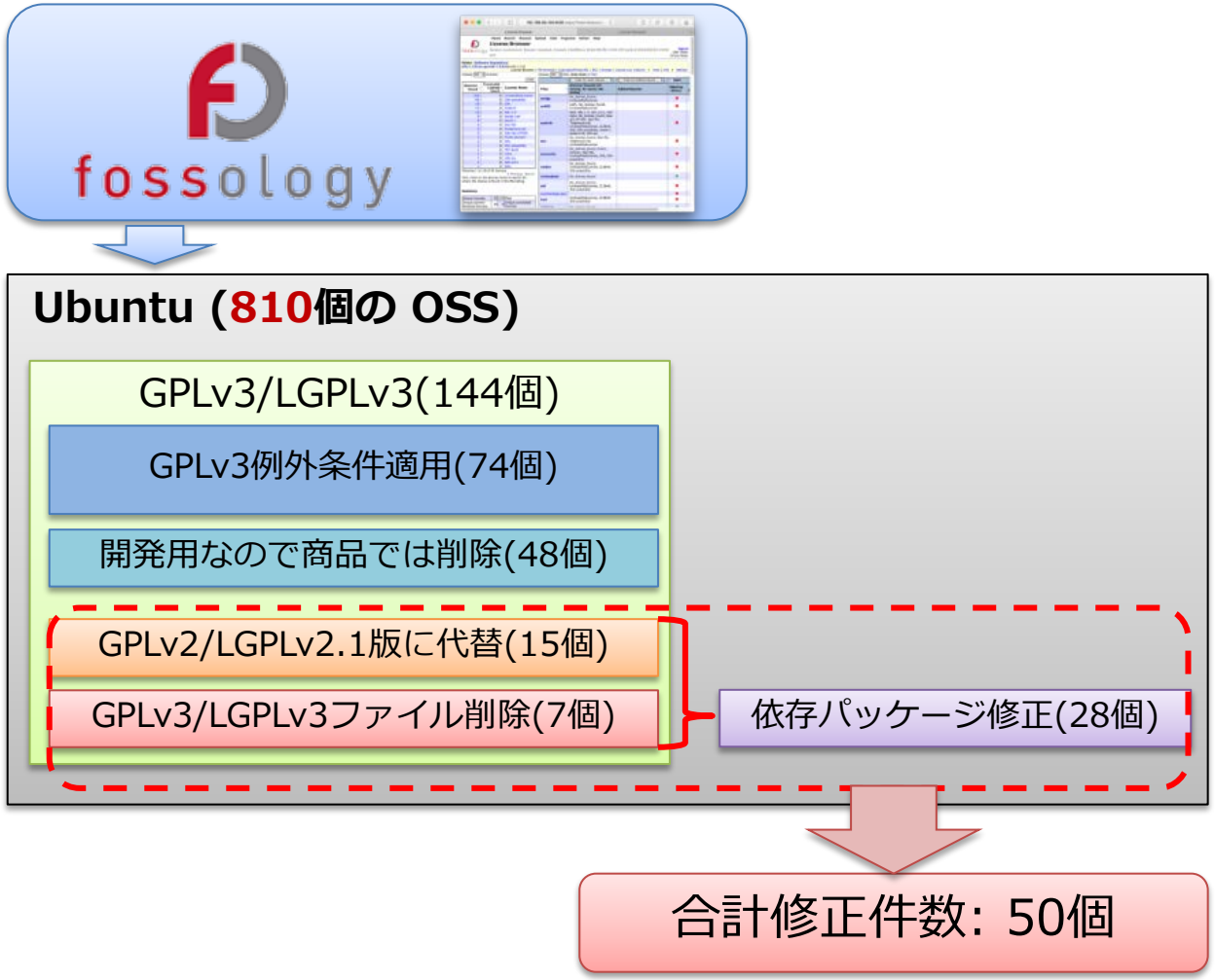
上位10ライセンスで OSS 全体の90% を占める

https://www.blackducksoftware.com/top-open-source-licenses

Agenda

- **自己紹介**
- **概要**
- **背景・前提**
  - OSS ライセンスとは
  - OSS ライセンストップ10
- **本題**
  - Sony 機器向け Linux における OSS のライセンス対応(GPLv3/LGPLv3)
  - FOSSology とは
  - FOSSology によるライセンス調査の実際
  - FOSSology で GPLv2 な OSS に GPLv3 ファイル混入を見つけたケース
- **まとめ**

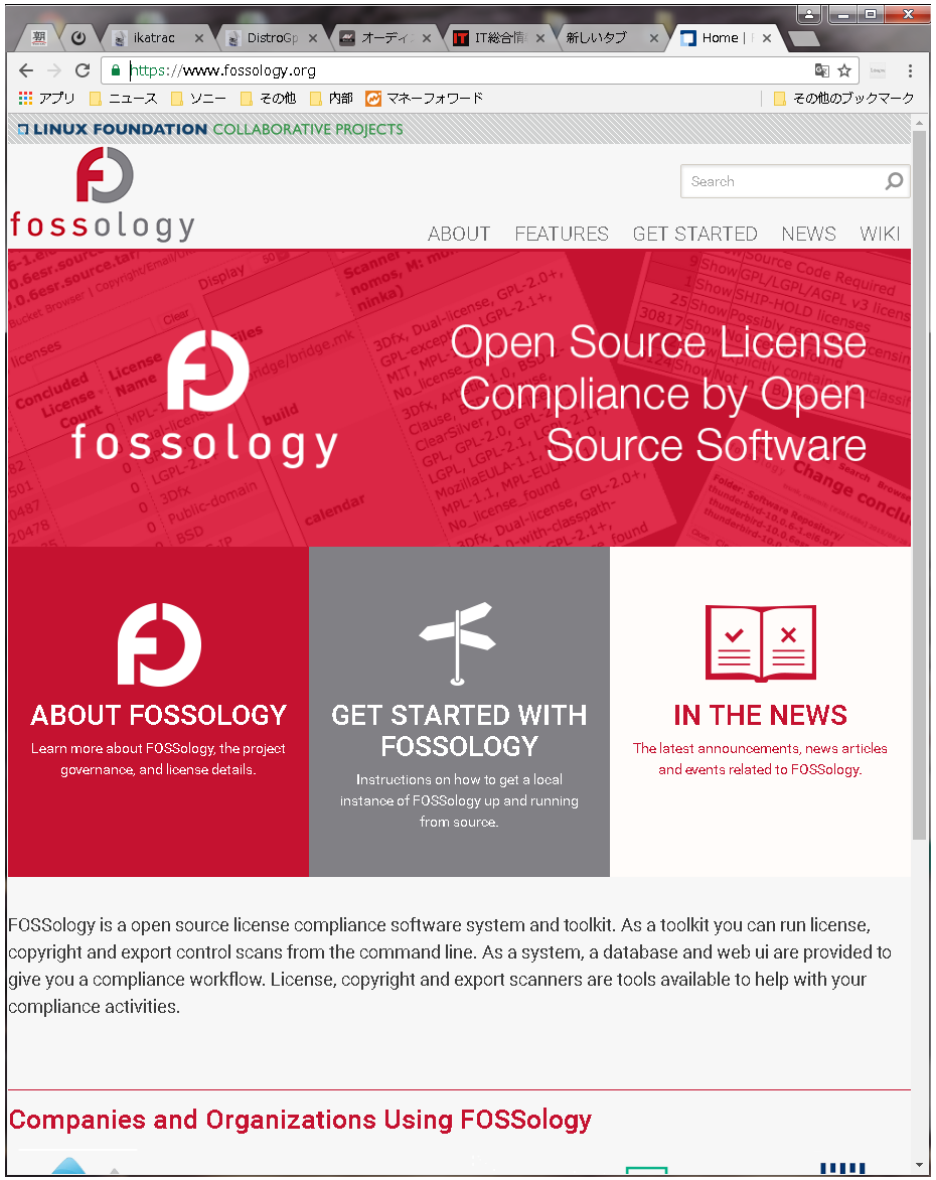
Sony 機器向け Linux における OSS のライセンス対応 (GPLv3/LGPLv3)



FOSSology とは

FOSSology ホームページ

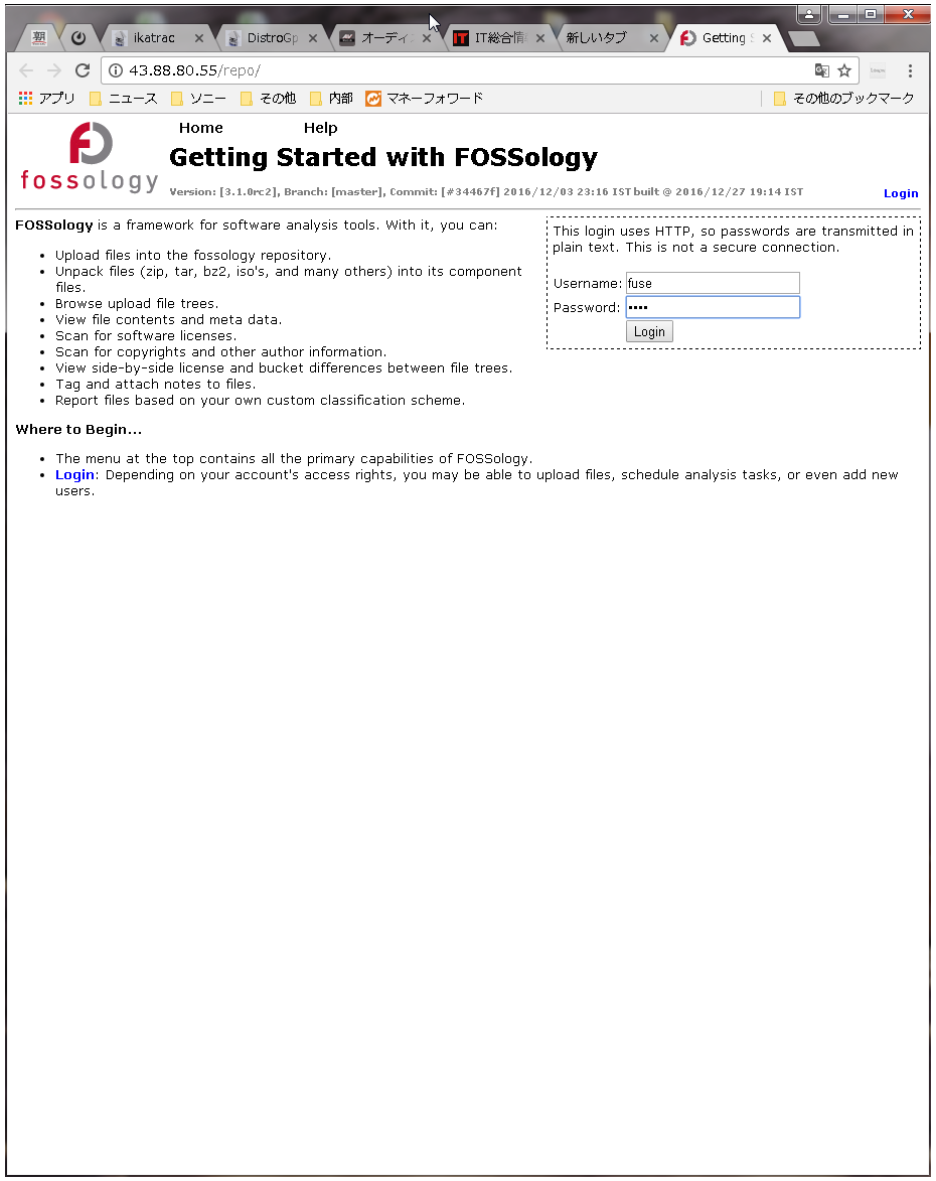
- ソフトウェアのライセンスや著作権情報を検出できる
  - FOSSology も無料のOSS ツールです。
- HP が中心で開発が行われ 2007 年から GPLv2 で公開している
- 現在 3.1.0 が最新
- FOSSology のドキュメント
  - https://www.linuxfoundation.jp/sites/mainjp/files/JP_lf_foss_compliance_fossology.pdf



FOSSology によるライセンス調査の実際

FOSSology トップページ

- FOSSology をインストール後、Web ブラウザでサーバをアクセス
- 管理者が設定した名前とパスワードでログイン

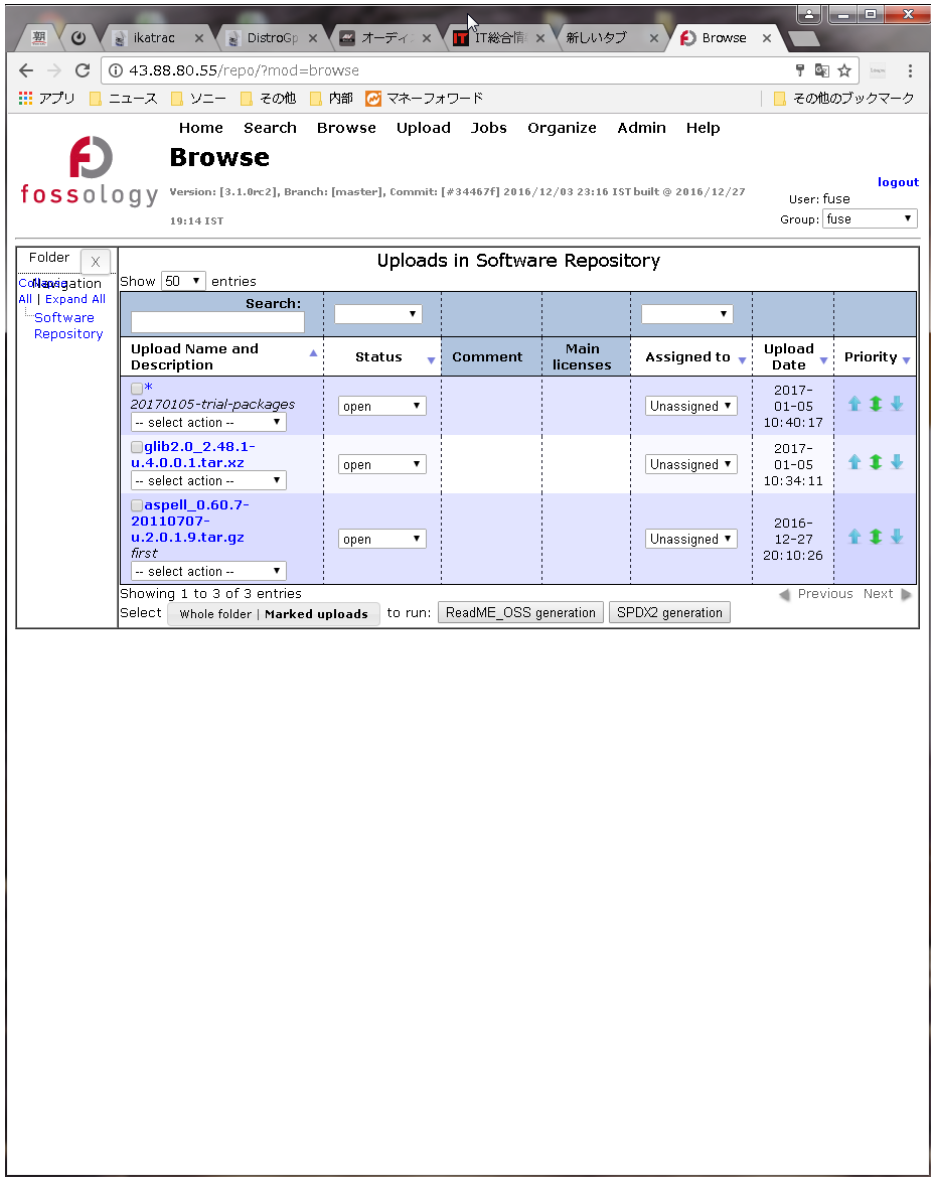


FOSSology によるライセンス調査の実際

FOSSology ブラウズページ

- ログインするとブラウズ画面に遷移する(遷移しない場合は上部の Browse をクリック)

- FOSSology サーバに登録されている OSS の一覧が表示される

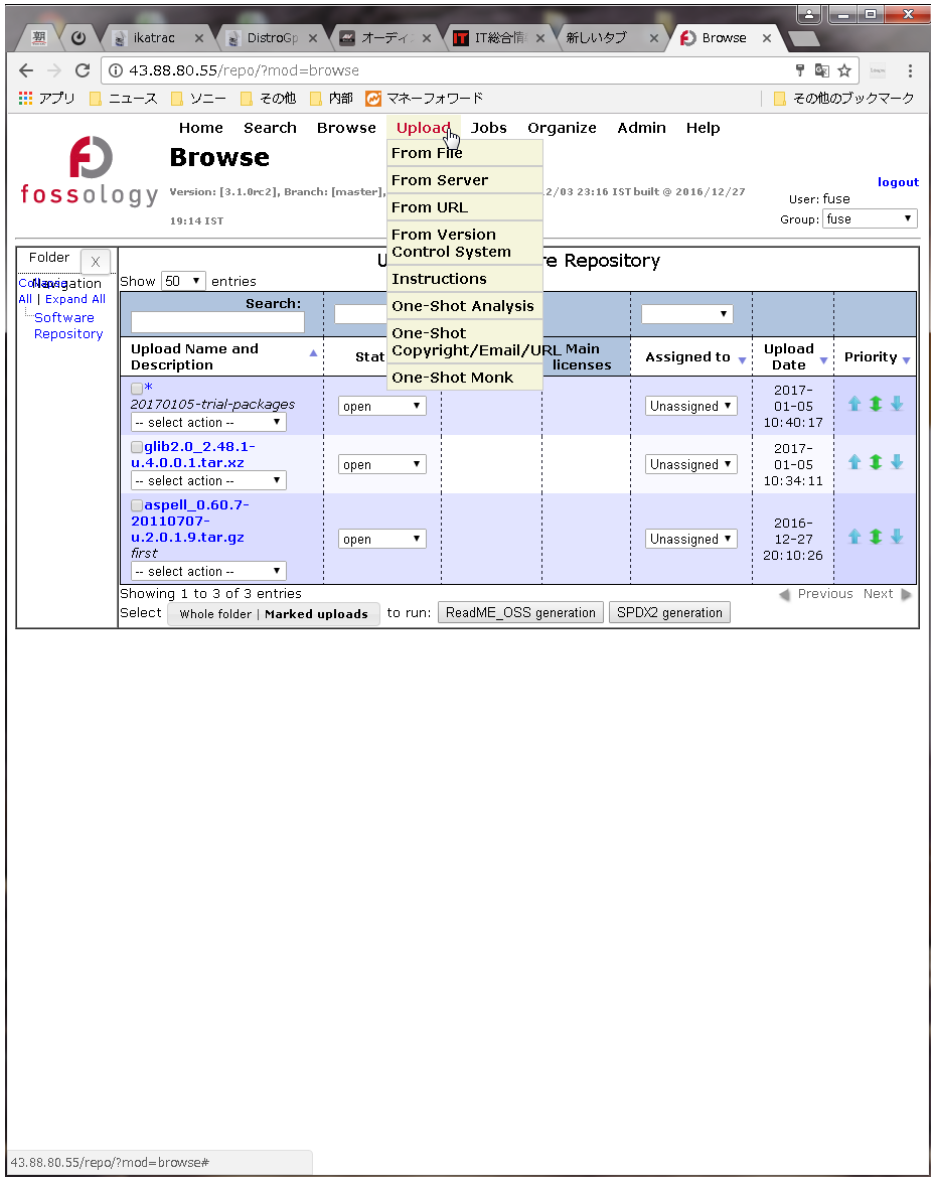


FOSSology によるライセンス調査の実際

FOSSology ブラウズページ

- ライセンス情報を確認したい OSS を FOSSology サーバに Upload する

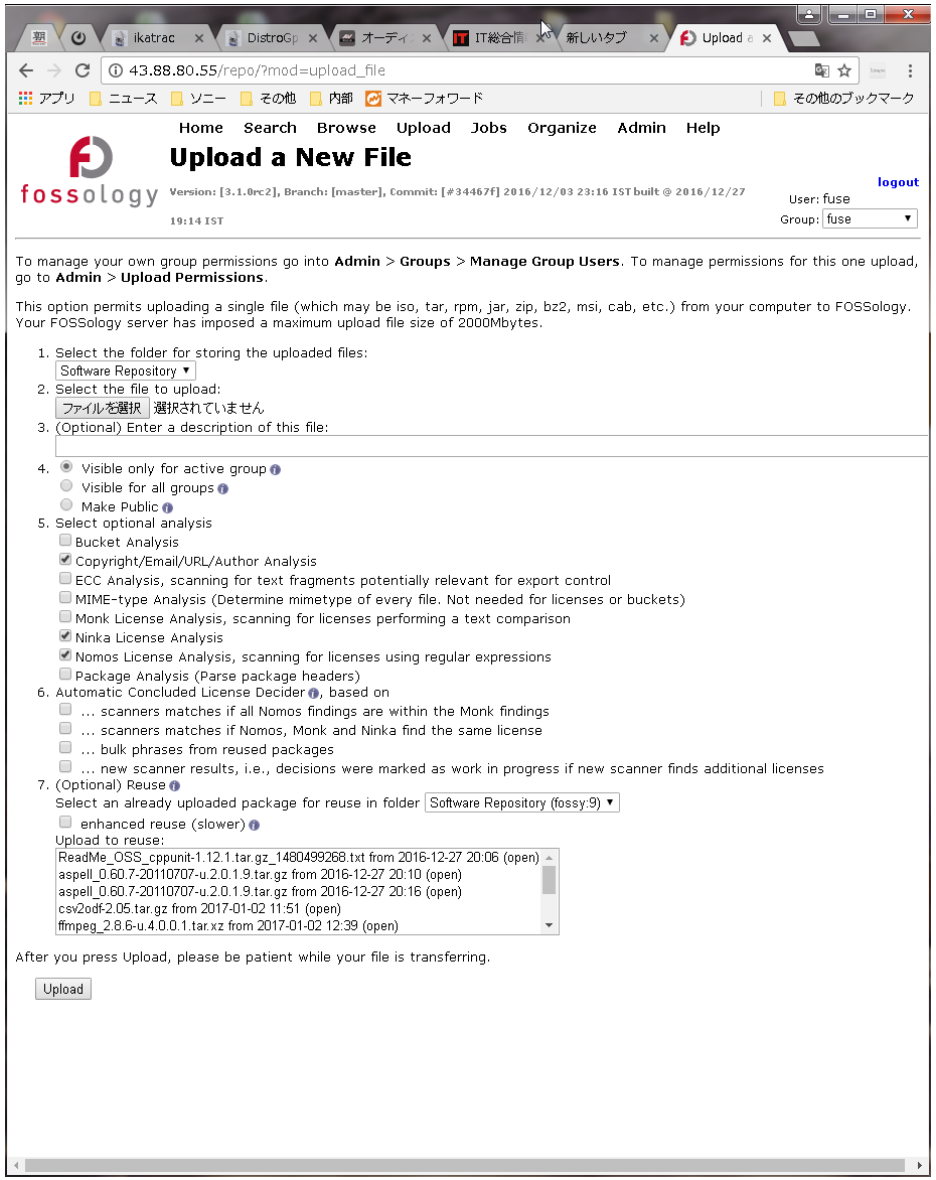
- Upload メニューから適当な方法を選択する。今回はソースコードをまとめたアーカイブファイルを指定するので From File を選択する。



FOSSology によるライセンス調査の実際

FOSSology Upload ページ

- Upload a New File 画面に遷移する
- 2. の ファイルを選択 ボタンを押して、Upload する OSS ソースアーカイブを指定する(今回は sed)
- Upload 時に自動的に行う解析を選ぶことができる。今回はデフォルトの状態にしておく
- 画面下の Upload ボタンを押すと処理がはじまる

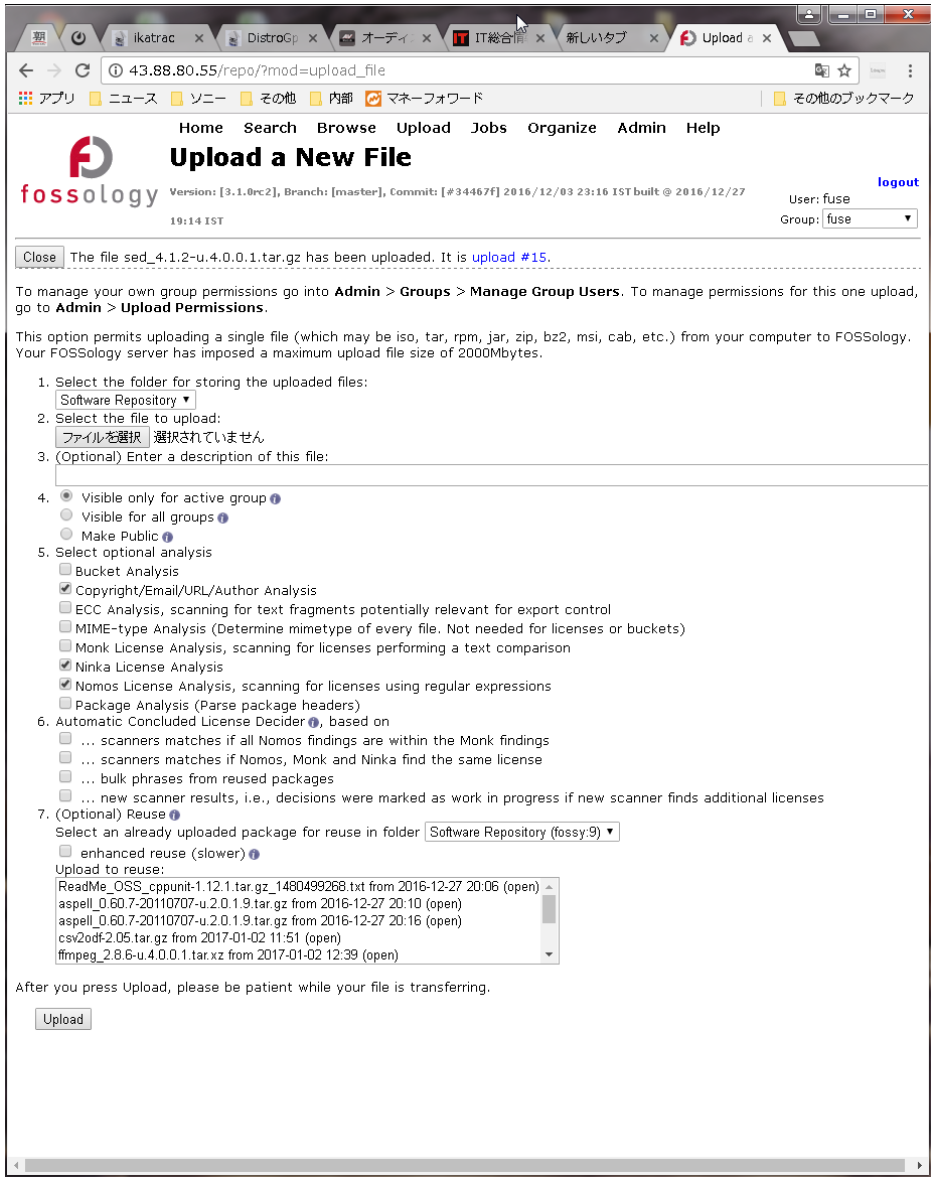


FOSSology によるライセンス調査の実際

FOSSology ブラウズページ

- 画面の上部に “The file sed_4.1.2_u.4.0.0.1.tar.gz has been uploaded. It is upload #15” の行が現れる。

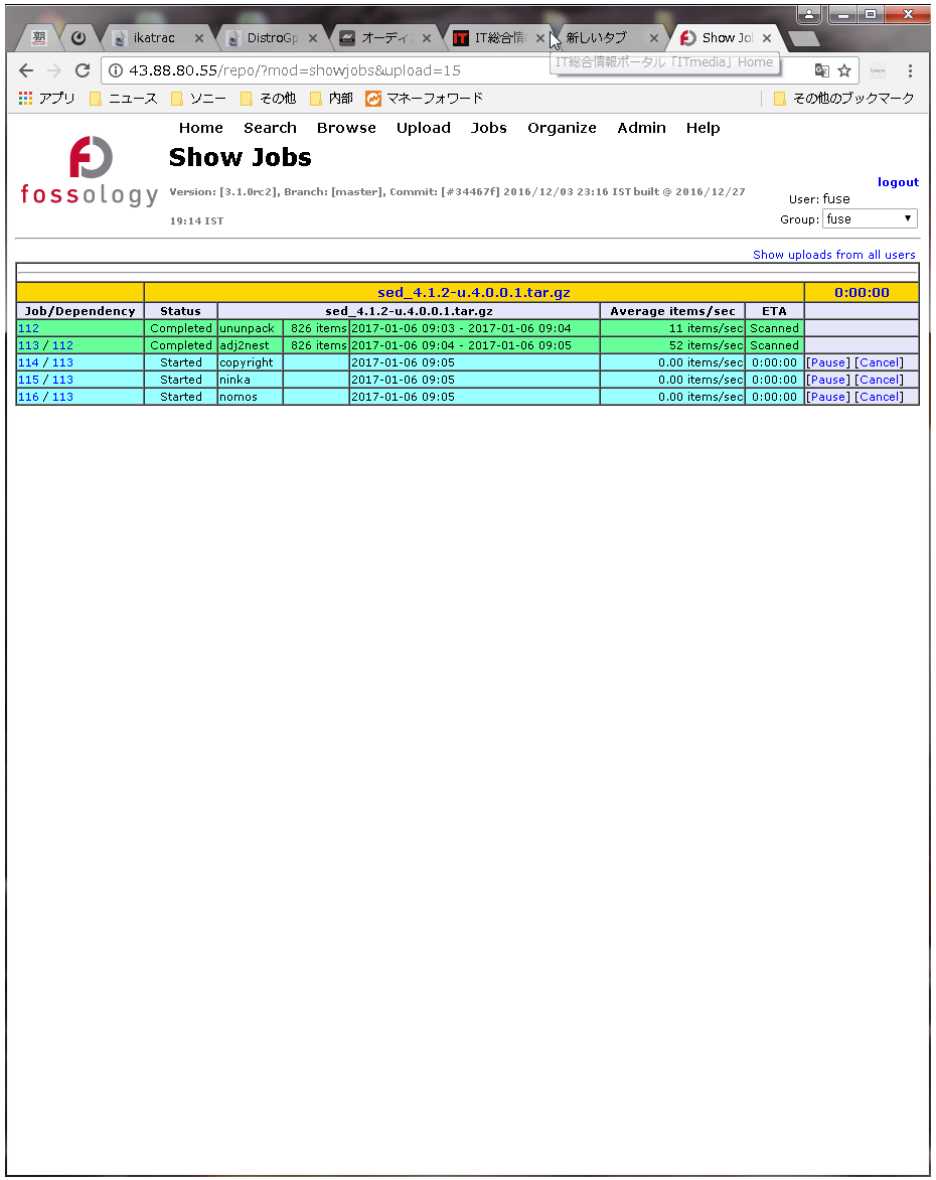
- upload #15 のリンクをクリックする



FOSSology によるライセンス調査の実際

FOSSology Show Jobs ページ

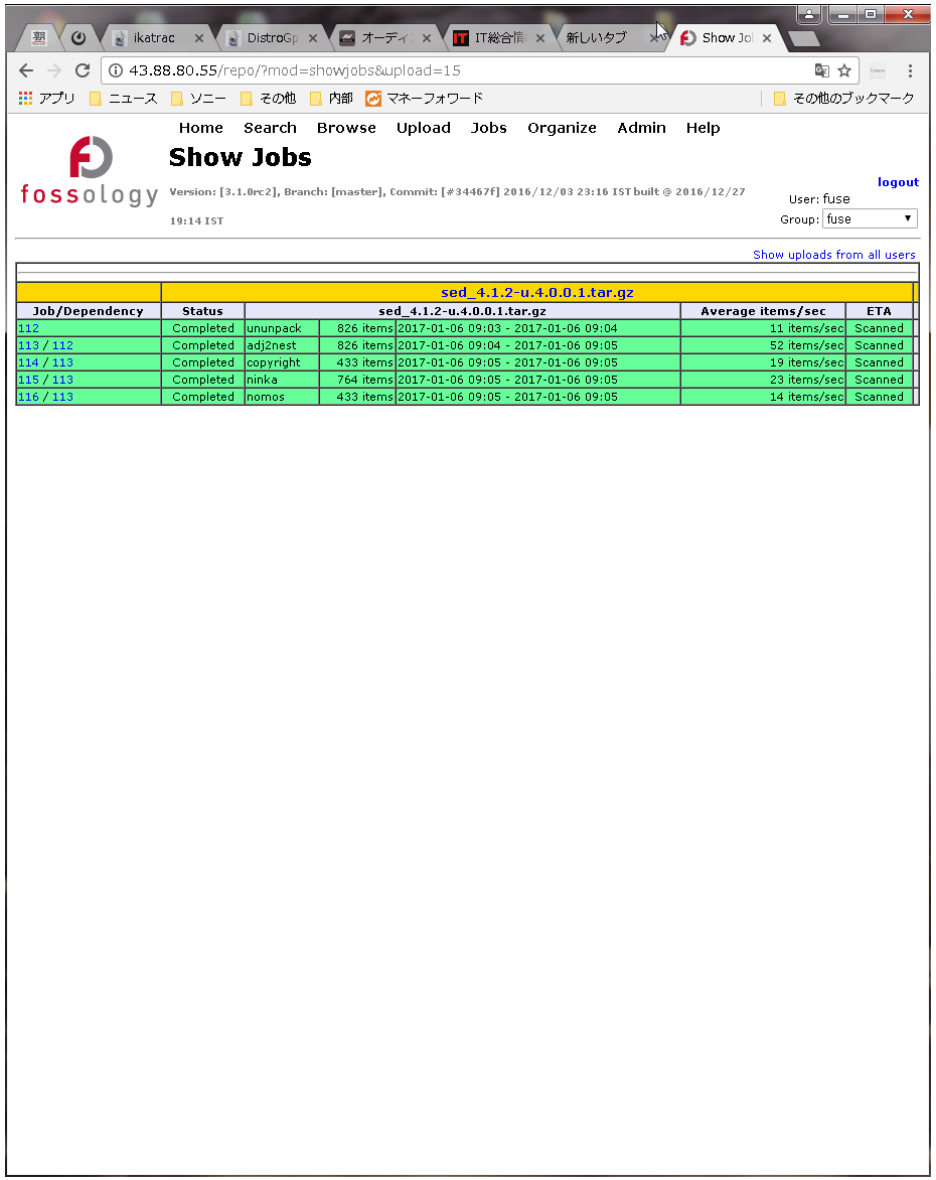
- 指定された sed の解析状況が表示される
- すべての Status が Completed になるまで待つ



FOSSology によるライセンス調査の実際

FOSSology Show Jobs ページ

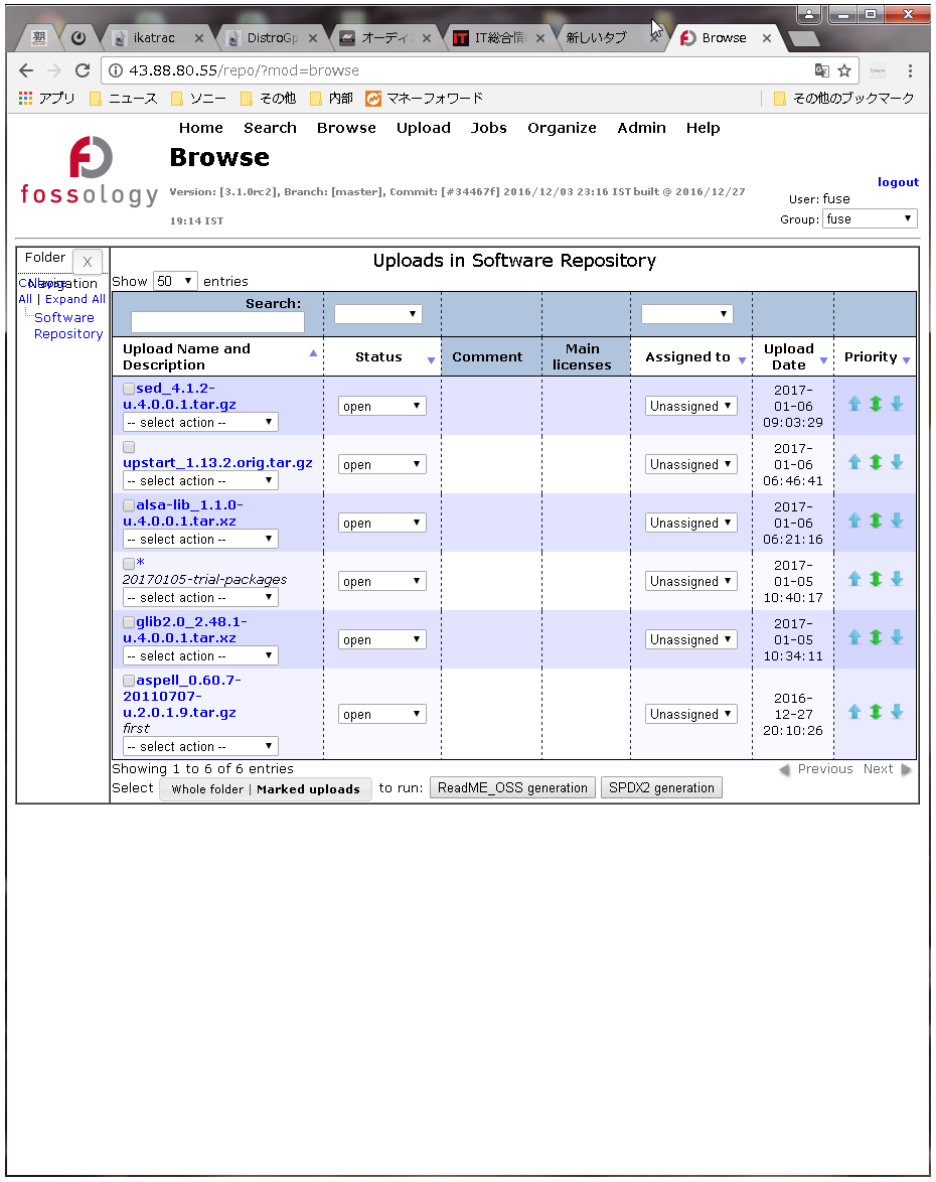
- すべての Status が Completed になったら解析終了なので Brows ボタンをおして Brows 画面に戻る



FOSSology によるライセンス調査の実際

FOSSology ブラウズページ

- 今 Upload した sed が新たな行として追加された。
- sed_4.1.2_u.4.0.0.1.tar.gz のリンクをクリックする



FOSSology によるライセンス調査の実際

FOSSology ブラウズページ

- sed のライセンス解析結果が表示される
- 画面左側が、ライセンス毎のファイル数である。
- 画面右側には、sed アーカイブファイルを展開した ディレクトリとファイルのリストが表示される。ディレクトリの場合は、中にあるファイルのライセンス一覧が表示される。ファイルの場合はそのファイルのライセンスが表示される
- 画面左側の GPL-2.0+ をクリックする

FOSSology によるライセンス調査の実際

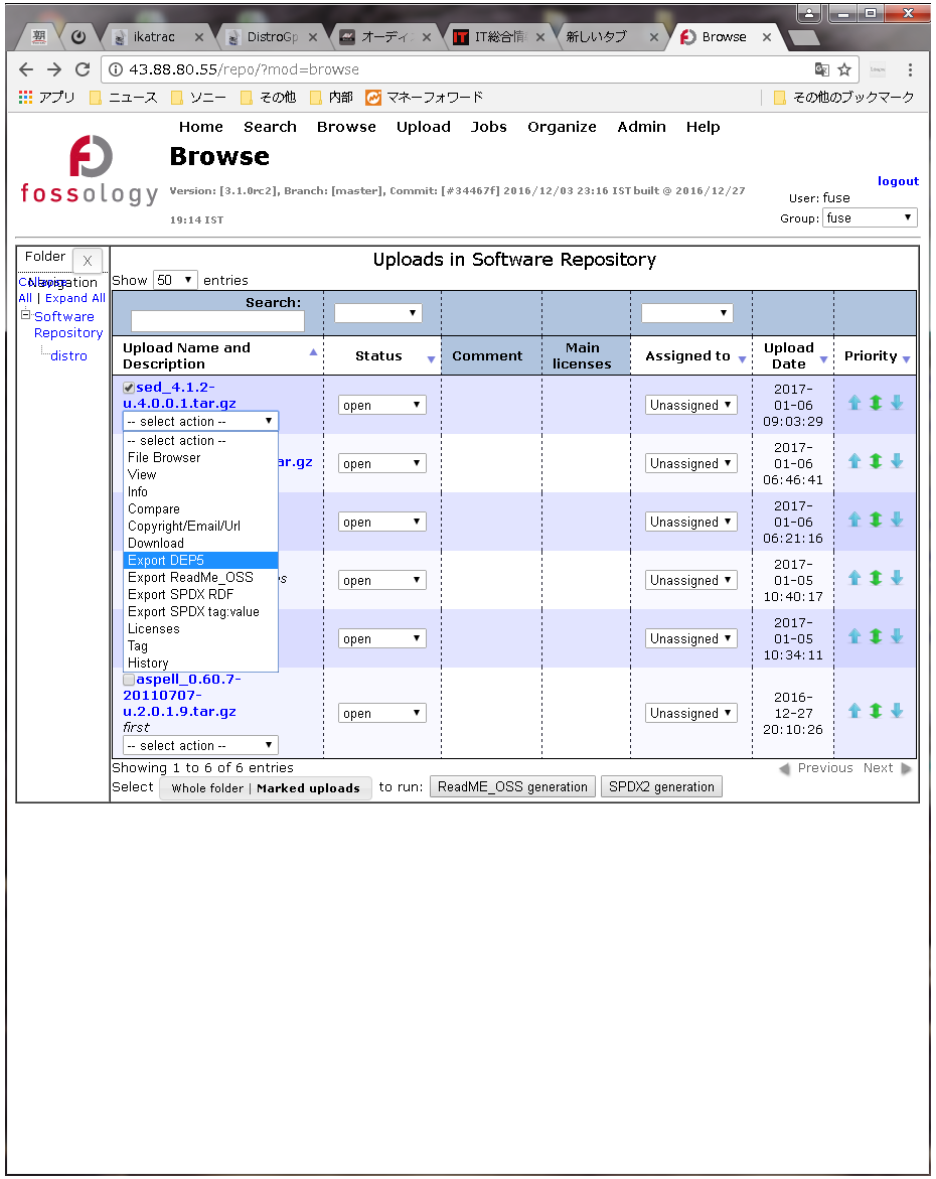
FOSSology ブラウズページ

- sed のソースコードのうち GPLv2 と判断されたファイルの一覧が表示される。

FOSSology によるライセンス調査の実際

FOSSology ブラウズページ

- sed のソースコードを選択して – select action – メニューから “Export DEP5” を選ぶ
- DEP5 とは Debian の Copyright フォーマットのこと
  - https://www.debian.org/doc/packaging-manuals/copyright-format/1.0/
- sed の DEP5 形式ファイルが生成される



FOSSology によるライセンス調査の実際

```
Format: http://www.debian.org/doc/packaging-manuals/copyright-format/1.0/
Upstream-Name: /srv/fossology/repository/report
Upstream-Contact:
Source:
Disclaimer: <text> This file is offered as-is, without any warranty. </text>
Copyright:
License:
Comment:  created on 2017-01-11T14:21:29Z with FOSSology

Files: sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/debian/{arch}/sed-debian/sed-debian--debian/sed-debian--debian--0/schizo@debian.org--2004-primary/patch-log/base-0
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/debian/{arch}/sed-debian/sed-debian--debian/sed-debian--debian--0/schizo@debian.org--2004-primary/patch-log/patch-17
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/debian/rules
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/debian/my/sedfaq.txt
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/COPYING
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/INSTALL
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/Makefile.in
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/doc/Makefile.in
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/doc/sed.texi
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/doc/sed.1
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/doc/sed-in.texi
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/config/help2man
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/config/texinfo.tex
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/config/texi2dvi
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/config/depcomp
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/config/strverscmp.m4
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/config/mdate-sh
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/config/install-sh
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/config/config.guess
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/config/missing
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/config/config.sub
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/config/stdbool.m4
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/config/config.rpath
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/aclocal.m4
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/lib/strerror.c
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/lib/obstack.h
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/lib/memcmp.c
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/lib/regexec.c
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/lib/regex_internal.c
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/lib/Makefile.in
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/lib/regex.c
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/lib/memmove.c
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/lib/strverscmp.c
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/lib/regcomp.c
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/lib/utils.c
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/lib/getopt1.c
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/lib/utils.h
       sed_4.1.2-u.4.0.0.1.tar.gz/sed_4.1.2-u.4.0.0.1.tar/sed-4.1.2/lib/regex_.h
```

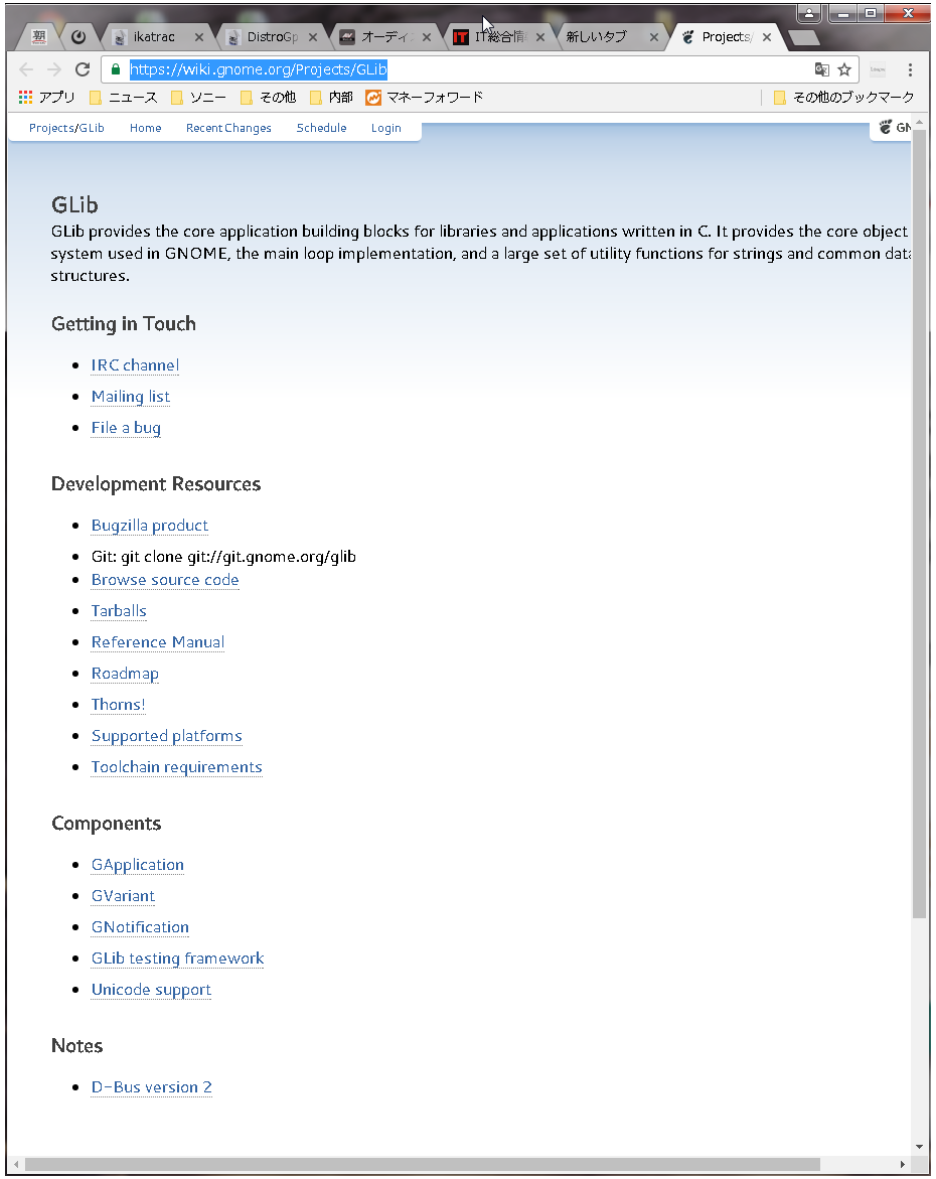
34行: 79桁 標準 UTF-8N LF 挿入

FOSSology で GPLv2 な OSS に GPLv3 ファイル混入を見つけたケース

Glib

- アプリケーションを作成する際によく使用されるストリング処理、線形リスト、ツリー、ログ機能やメモリ管理などの基本的な機能、 字句解析機能や、イベントドリブン機構などが詰まったライブラリ

- ライセンスは **LGPLv2**
  - https://developer.gnome.org/glib/stable/glib.html
  - https://github.com/GNOME/glib/blob/master/COPYING



FOSSology による GPLv3 ファイルの検出 (glib)

- **glib のソースコードに GPLv3 ファイルが存在**
  - config.guess: autoconf exception 3.0 (問題なし)
  - config.sub: autoconf exception 3.0 (問題なし)
  - ltmain.sh: libtool exception (問題なし)
    - https://spdx.org/licenses/exceptions-index.html
  - glib/gnu/lib/verify.h: GPLv3 汚染

Glib 開発コミュニティに連絡

>> I found GPLv3 header file in glib 2.48
>> https://github.com/GNOME/glib/blob/master/glib/gnulib/verify.h

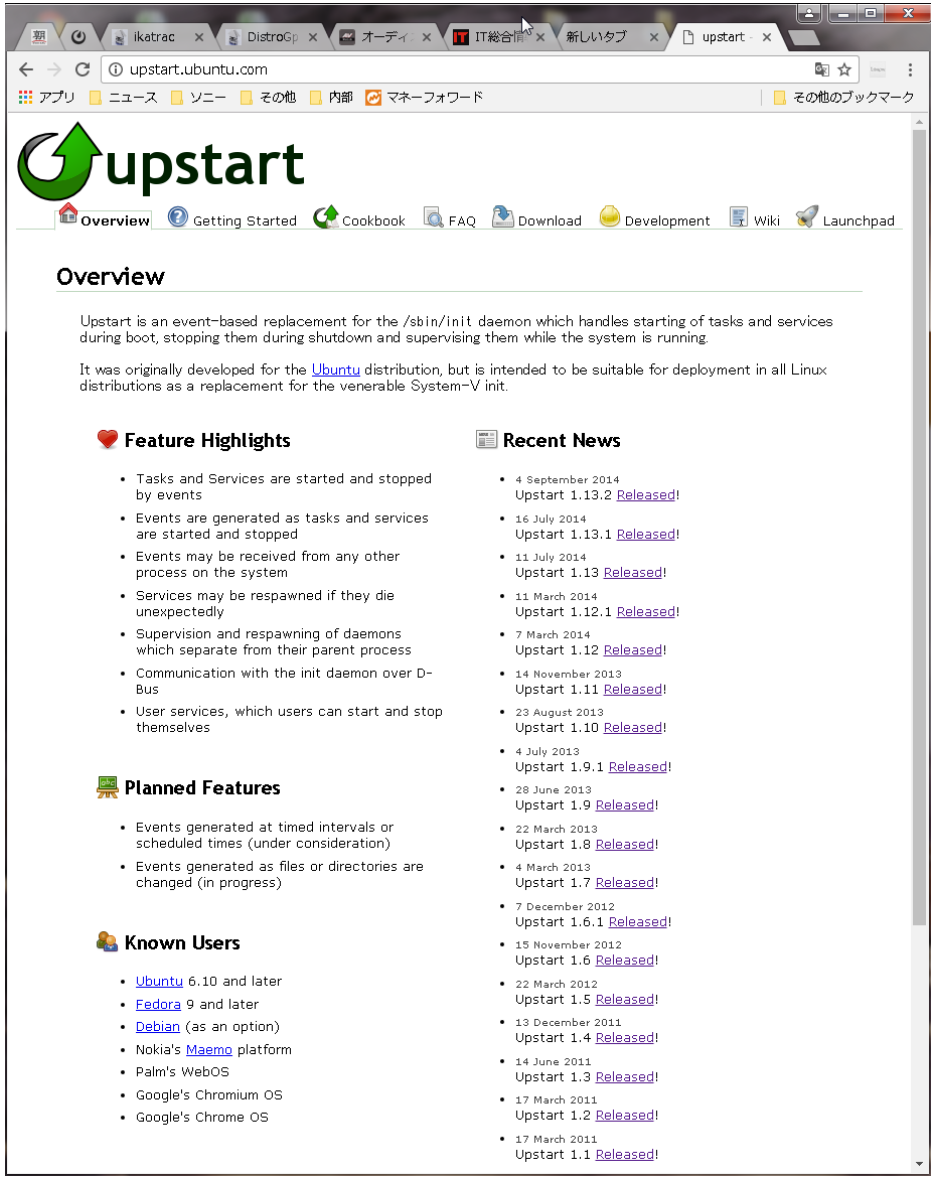
This is a mistake made by the person who was the last to update vasnprintf module in glib. gnulib-tool has --lgpl=2 flag, which will substitute the license in the headers, including verify.h, making them LGPLv2.1+

So i'd say that we're factually in the clear, just need to fix the licensing information in verify.h

解決

Upstart

- Ubuntu で使われている /sbin/init 置き換えデーモン
- ライセンスは GPLv2
  - http://bazaar.launchpad.net/~upstart-devel/upstart/trunk/view/head:/COPYING



FOSSology による GPLv3 ファイルの検出 (upstart)

- **upstart のソースコードに GPLv3 ファイルが存在**
  - ChangeLog: 誤検出
  - NEWS: 誤検出
  - test_conf_preload.sh.in:
    - テスト用スクリプト
    - バイナリパッケージには含まれないので問題なし
  - run_abi_checker.sh.in:
    - ABI チェック用スクリプト
    - バイナリパッケージには含まれないので問題なし
  - init-checkconf.sh:
    - Upstart 設定ファイルチェック用スクリプト
    - バイナリパッケージに含まれているので GPLv3 汚染

バイナリパッケージから削除することで対応

Agenda

- **自己紹介**
- **概要**
- **背景・前提**
  - OSS ライセンスとは
  - OSS ライセンストップ10
- **本題**
  - Sony 機器向け Linux における OSS のライセンス対応(GPLv3/LGPLv3)
  - FOSSology とは
  - FOSSology によるライセンス調査の実際
  - FOSSology で GPLv2 な OSS に GPLv3 ファイル混入を見つけたケース
- **まとめ**

まとめ

- OSS を取り扱う上で必要なライセンスに関する背景・前提を説明した
- Sony 機器向け Linux における OSS ライセンス対応(特に GPLv3/LGPLv3 混入対策)について説明した